Academic Excellence Through Quality Education

KATHMANDU MODEL SECONDARY SCHOOL

PROJECT WORK ON

NEURAL NETWORKING

&

CYBER SECURITY

Submitted To: Gaurav Mishra

(Department of Computer Science, KMSS Bagbazar)

Team members:

1. Ujjwal Agrahari (Reg. no. 77760131J)
2. Sanjeev Jaiswal (Reg. no. 77760158F)
3. Apil Raj Acharya (Reg. no. 777601262)

PREFACE

The simplest definition of a neural network, more properly referred to as an 'artificial' neural network (**ANN**), is provided by the inventor of one of the first neurocomputers, Dr. Robert Hecht-Nielsen. He defines a neural network as:
"...a computing system made up of several simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs".

ANNs are processing devices (algorithms or actual hardware) that are loosely modeled after the neuronal structure of the mammalian cerebral cortex but on much smaller scales. Computations are made by the processor reading an instruction as well as any data the instruction requires from memory addresses, the instruction is then executed and the results are saved in a specified memory location as required. Application areas include system identification and control like vehicle control, trajectory prediction, process control, natural resources management, quantum chemistry, general game playing, pattern recognition, radar systems, face identification, signal classification, 3D reconstruction, visual perception, sequence recognition, gesture, speech, handwritten and printed text recognition, diagnosis, finance. E.g automated trading systems, data processing, visualization, MT, social network filtering, and e-mail spam filtering.

Moreover, under this project, we bring the hot topic regarding cybercrime, possible threats under it, and the way to defend it through cyber security. Computer security, cybersecurity or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

There are different cyber-crimes committed that have driven the internet in its misuse. Therefore, we all need to be careful using Internet services and secure our privacy. It is also our duty to fight against these activities. We hope this project can be helpful for every individual to develop brief knowledge in "*Neural Networks*" and "*Cyber Security*."

Group Members

ACKNOWLEDGEMENT

It is always a pleasure to remind fine people in valuable project works. The success and final outcome of this project required a lot of guidance and assistance from many people and we're extremely privileged to have got this all along the completion of my project. All that we have done is only due to such supervision and assistance and we would not forget to thank them.

Firstly, we're highly indebted to our Computer Science teacher **Mr. Gaurav Mishra** for his guidance and constant supervision as well as for providing necessary information regarding the project & also for his support in completing the project.

We're equally thankful to KMC College and the lab teachers for providing the internet and other facilities for research that we also used in the continuous testing of our codes and debugging them if necessary.

Many people, especially our classmates and team members themselves, have made valuable comments and suggestions on this proposal which gave us the inspiration to improve our assignment. We thank all the people for their help directly and indirectly to complete our assignment.

Contents

Neural Networking:

Cyber Secrecy:

List of Figures

Neural Networks

Introduction

Neural networks are a gaggle of algorithms, modeled loosely after the human brain, that are designed to acknowledge patterns. They interpret sensory data through a kind of machine perception, labeling or clustering raw input. The patterns they recognize are numerical contained in vectors, into which all real-world data, images, sound, text or statistic, must be translated.

It is a series of algorithms that endeavors to acknowledge underlying relationships during a very set of data through a process that mimics the way the human brain operates. During this sense, neural networks ask systems of neurons, either organic or artificial in nature. Neural networks can adapt to changing input; therefore, the network generates the foremost effective possible result without having to revamp the output criteria. The concept of neural networks, which has its roots in computing, is swiftly gaining popularity within the event of trading systems. It is vaguely inspired by the biological neural networks that constitute animal brains.

Such systems learn to perform tasks by considering examples, generally without being programmed with task-specific rules. As an example, in image recognition, they'll learn to identify images that contain cats by analyzing example images that are manually labeled as "cat" or "no cat" and using the results to identify cats in other images. They're doing this with no prior knowledge of cats, for example, that they have fur, tails, whiskers, and cat-like faces.

Instead, they automatically generate identifying characteristics from the examples that they process. An ANN relies on a group of connected units or nodes called artificial neurons, which loosely model the neurons during a very biological brain. Each connection, a bit like the synapses during a very biological brain, can transmit a symbol to other neurons. A man-made neuron that receives a symbol then processes it and should signal neurons connected there.

In ANN implementations, the signal at a connection might be a posh quantity, and also the output of each neuron is computed by some non-linear function of the sum of its inputs. The connections are called edges. Neurons and edges typically have a weight that adjusts as learning proceeds. The burden increases or decreases the strength of the signal at a connection.

Neurons may have a threshold specified a symbol is distributed as long as the mixture signal crosses that threshold. Typically, neurons are aggregated into layers. Different layers may perform different transformations on their inputs. Signals travel from the first layer (the input layer), to the last layer (the output layer), possibly after traversing the layers multiple times.

History

The study of the human brain is thousands of years old. With the looks of recent electronics, it had been only natural to undertake to harness this thinking process. The first step toward artificial neural networks came in 1943 when Warren McCulloch, a neurophysiologist, and a young mathematician, Walter Pitts, wrote a paper on how neurons might work. They modeled an easy neural network with electrical circuits. As computers advanced into their infancy of the 1950s, it became possible to start out to model the rudiments of these theories concerning human thought. Nathanial Rochester from the IBM research laboratories led the first effort to simulate a neural network. That first attempt failed. But later attempts were successful.
It had been during now that traditional computing began to flower and, as it did, the strain in computing left the neural research within the background.

In 1970, Seppo Linnainmaa published the general method for automatic differentiation (AD) of discrete connected networks of nested differentiable functions. In 1973, Dreyfus used backpropagation to adapt parameters of controllers in proportion to error gradients. Werbos's (1975) backpropagation algorithm enabled practical training of multi-layer networks. In 1982, he applied Linnainmaa's AD method to neural networks within the way that became widely used. Thereafter research stagnated following Minsky and Papert (1969), who discovered that basic perceptron were incapable of processing the exclusive-or circuit which computers lacked sufficient power to process useful neural networks.

The development of metal–oxide–semiconductor (MOS) very-large-scale integration (VLSI), within the type of complementary MOS (CMOS) technology, enabled the event of practical artificial neural networks within 1980s.

Models of Neural Networking

Neural networks are simple models of the way the nervous system operates. The essential units are neurons, which are typically organized into layers, as shown within the subsequent figure. A neural network is an integrated model of the way the human brain processes instructions.

Structure of a neural network

A neural network might be a simplified model of the way the human brain processes information. It works by simulating an outsized number of interconnected processing units that resemble abstract versions of neurons. The processing units are arranged in layers. There are typically three parts during a very neural network: an input layer, with units representing the input fields; one or more hidden layers; and an output layer, with a unit or units representing the target field.

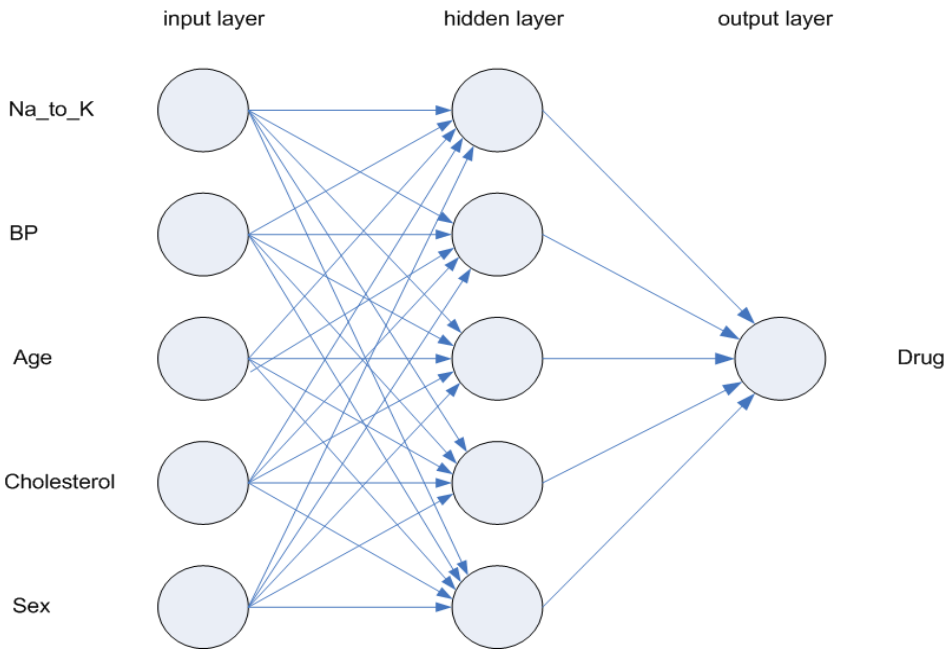

Figure 1: Structure of ANN

Working Prototype for Neural Networks

The units are connected with varying connection strengths (or weights), layer, and values are propagated. Input file are presented to the primary from each neuron to each neuron within the next layer. Eventually, a result is delivered from the output layer. The network learns by

examining individual records, generating a prediction for every record, and making adjustments to the weights whenever it makes an incorrect prediction. This process is repeated repeatedly, and therefore the network continues to enhance its predictions until one or more of the stopping criteria are met.

Initially, all weights are random, and therefore the answers that begin of internet are probably nonsensical. The network learns through training. Examples that the output is understood are repeatedly presented to the network, and therefore the answers it gives are compared to the known outcomes. Information from this comparison is passed back through the network, gradually changing the weights. As training progresses, the network becomes increasingly accurate in replicating the known outcomes. Once trained, the networks are often applied to future cases where the result is unknown.

The following figure show represents the model of artificial neural networks:

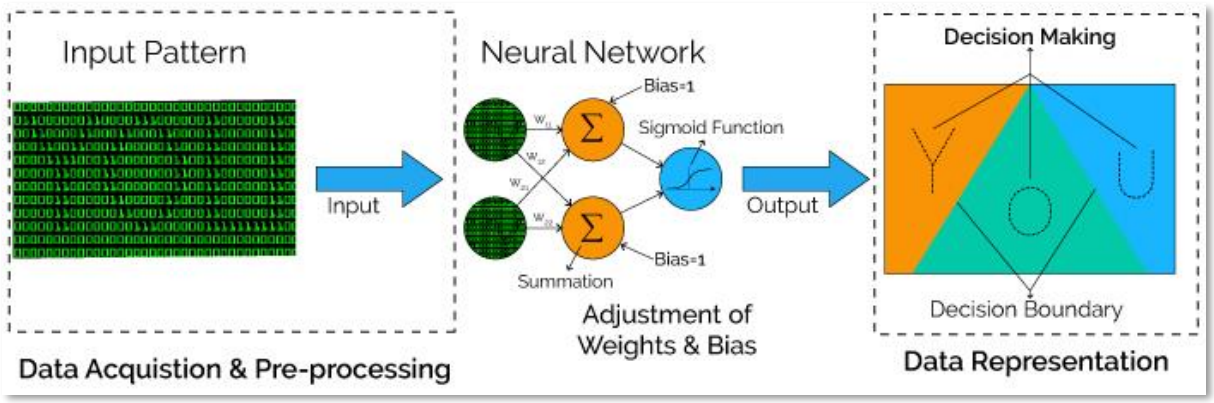

Figure 2: Model of ANN

Components of Neural Networking:

Neural systems are explicitly structured dependent on the internal functions of biological brains. These models impersonate the elements of interconnected neurons by going information includes through a few layers of what are alluded to as **perceptron** (might suspect 'neurons'), each changing the information utilizing a lot of capacities.

The following explanation clarifies the components of a perceptron, the littlest segment of a neural system.

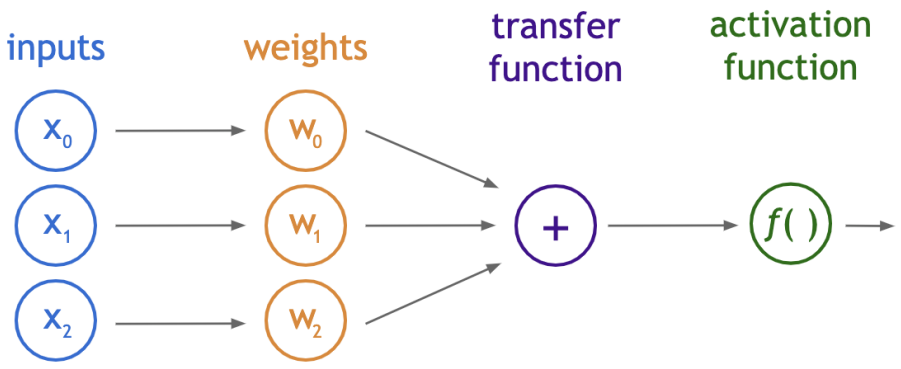

Figure 3: Structure of Perceptron

A perceptron (above) is commonly comprised of three principle math tasks: scalar multiplication, a summation, and then a transformation using a distinct equation called an **activation function**. Since a perceptron represents a single neuron in the brain, we can put together many perceptrons to represent a brain. That would be called a neural network, but more on that later.

i. **Inputs:** The inputs are simply the measures of our features. For a single soil sample, this would be an array of values for each measurement. For example, we may have an input of:

$$[\ 58\ ,\ 1.3\ ,\ 11\ ]$$

showing 58% moisture, 1.3mm grain size, and 11 micrograms iron per kg soil weight. These inputs are what will be modified by the perceptron. The above example clears about this component.

ii. **Weights:** Weights represent scalar multiplications. Their job is to assess the importance of each input, as well as directionality. For example, does more iron contribute too much or a small to height? Does it make the tree taller or shorter? Getting these weights right may be a very difficult task, and there are many various values to undertake.

iii. **Transfer Function:** The transfer function is different from the other components in which it takes multiple inputs. The job of the transfer function is to combine multiple inputs into one output value so that the activation function can be applied. This is usually done with an easy summation of all the inputs to the transfer function.

$$11.6 + 12.48 + -9.9 = 14.18$$

This scalar value is supposed to represent some information about the soil composition. This value has already factored in the importance of each measurement, using the weights. Now it is a single value that we can actually use. You can almost think of this as an arbitrary weighted index of the soil's components. If we've tons of those indexes, it'd become easier to predict tree height using them. Before the worth is shipped out of the perceptron because the final output, however, it's transformed using an activation function.

iv. **Activation Function:** Activation Function: An activation function will transform the number from the transfer function into a value that overemphasizes the input. Often times, the activation function will be non-linear. Introducing non-linearity to the perceptron helps avoid the output varying linearly with the inputs and thus allows for greater complexity to the model. Below are two common activation functions.

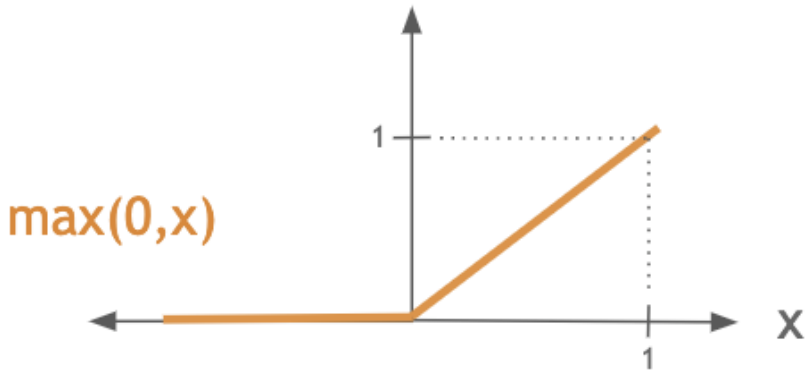

Figure 4: Activation function

ReLU is a simple function that compares zero with the input and picks the maximum. That means that any negative input comes out as zero, while positive inputs are unaffected. This is useful in situations where negative values don't make much sense, or for removing linearity without having to do any heavy computations.

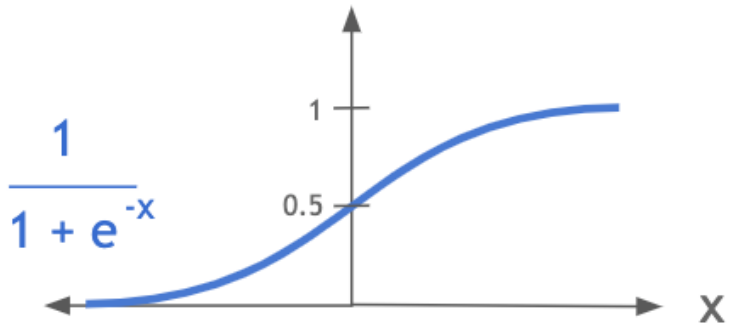

Figure 5: ReLU function

The sigmoid function does a good job of separating values into different thresholds. It is particularly useful for values like z-scores, where values towards the mean (zero) got to be checked out carefully since a little change near the mean may significantly affect a selected behavior, but where values far away from the mean probably indicate an equivalent thing about the info. For example, if soil has lots and lots of moisture, a small addition to moisture probably won't affect tree's height, but if it has a very average level of moisture then removing some bit of moisture could affect the tree height significantly. It emphasizes the difference in values if they're closer to zero.

Remember that it's a nonlinear function that makes the input more dramatic. That is, inputs closer to zero are typically affected quite inputs distant from zero. It basically forces values like 4 and 4.1 to be much closer, while values like 0 and 0.1 become more spread apart. The purpose of this is often to permit us to select more distinct decision boundaries. If, for instance , we try to classify a tree as either "tall," "medium," or "short," values of 5 or -5 are very obviously representing tall and short. But what about values like 1.5? Around these numbers, it may be more difficult to determine a decision boundary, so by dramatizing the input it may be easier to split the three categories.

We pick an activation function before training our model, so the function itself is always the same. It is not one among the parameters we toggle when testing thousands of various models.

Learning and Learning Paradigms

Learning:

Learning is the adaptation of the network raised to handle a task by considering sample observations. Learning involves adjusting the weights (and optional thresholds) of the network to enhance the accuracy of the result. This is done by minimizing the observed errors.

Learning Paradigms:

The ways used to teach the machine how to behave like the biological system are called as the learning paradigms. The three learning paradigms in neural networks are supervised, unsupervised, and reinforcement learning:

1) **Supervised Learning:**

   The first and most elementary of the learning paradigms is supervised learning. In supervised learning, we've a really clear and defined goal to predict something using our data. In this manner, we usually use this approach to unravel problems of classification or regression.

   To use supervised learning, we require our data points to possess labels which tell us the right answer to the question that we proposed. We then take all our data and split it into testing data, which we hide, and training data which we use to coach our model. In this way, we are allowing the neural network to possess a solution key to the question it asks of our training data. The model will then find the optimal thanks to use the info to match that answer key. We can then evaluate how well our neural network performs on real-world data by allowing it to see the unseen test data and make predictions on it.

   Examples:

   - Predict housing prices
   - Detect spam
   - Face detection
   - Speech automated systems

2) **Unsupervised learning:**

   The second learning paradigm is unsupervised learning. This is a process that acts upon data without labels or target variables. In unsupervised learning, the goal is to get patterns and trends within a dataset then use those patterns to form predictions about new data. Within the context of a

neural network, the goal is to work out the organization of the dataset it's fed. Unsupervised Learning takes data and finds similarities between data points.

Examples:

- Market Segmentation
- Distinguishing shapes of cancerous cells
- Does a star exist in certain space?
- *Roomba* mapping

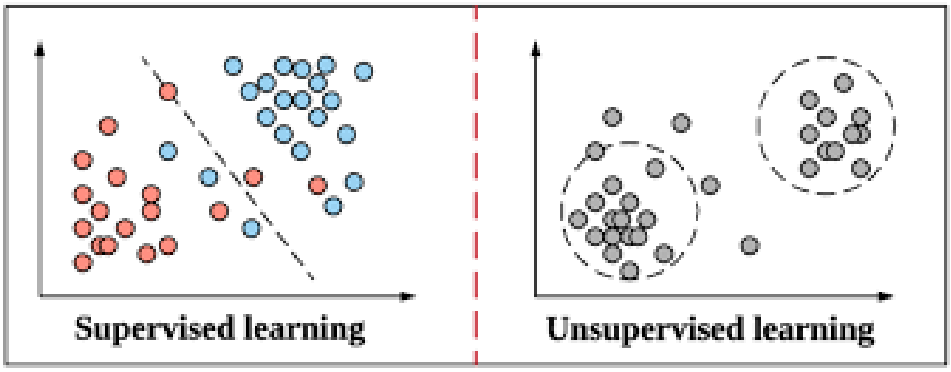

Figure 6: Comparison between supervised and unsupervised learning

3) **Reinforced learning:**

The final method of learning implemented in neural networks is reinforcement learning. This sort of learning is distinct from the opposite two because it's a selected goal that it's pushing the machine to maneuver towards. There is a selected outcome that's expected, the machine chooses and learns the foremost optimal path to realize it. The way this is often accomplished is through providing the machine with rewards and punishments supported their performances that culminate during a long-term end-goal. Rewards and punishment signals are only received by the machine when the machine achieves a replacement state. Instantaneous feedback isn't a neighborhood of this paradigm of learning.

Examples:

- Traffic Signal Control
- Robotics Control
- Games

The Types of Neural networks

There are ultimately seven types of artificial neural networks. They are briefly explained as follows:

i. **Feedforward Neural Network – Artificial Neuron**

This is one among the only sorts of artificial neural networks. In a feedforward neural network, the info passes through the various input nodes till it reaches the output node. In other words, data moves in just one direction from the primary tier onwards until it reaches the output node. This is also referred to as a front propagated wave which is typically achieved by employing a classifying activation function.

Unlike in additional complex sorts of neural networks, there's no backpropagation and data moves in one direction only. A feedforward neural network may have one layer or it's going to have hidden layers. In a feedforward neural network, the sum of the products of the inputs and their weights are calculated. This is then fed to the output. Here is an example of one layer feedforward neural network.

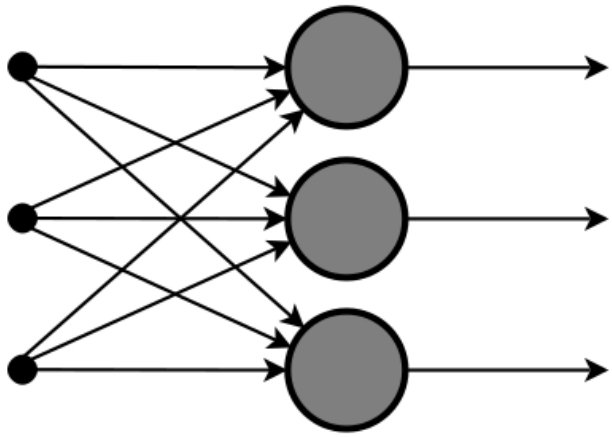

Figure 7: Feedforward Neural Network – Artificial Neuron

Feedforward neural networks are utilized in technologies like face recognition and computer vision. This is often because the target classes in these applications are hard to classify. A simple feedforward neural network is provided to affect data which contains tons of noise. Feedforward neural networks also are relatively simple to take care of.

ii. **Radial Basis Function Neural Network**

A radial basis function considers the space of any point relative to the centre. Such neural networks have two layers. Within the inner layer, the features are combined with the radial basis function. Then the output of those features is taken under consideration when calculating an

equivalent output within the next time-step. Here may be a diagram which represents a radial basis function neural network.

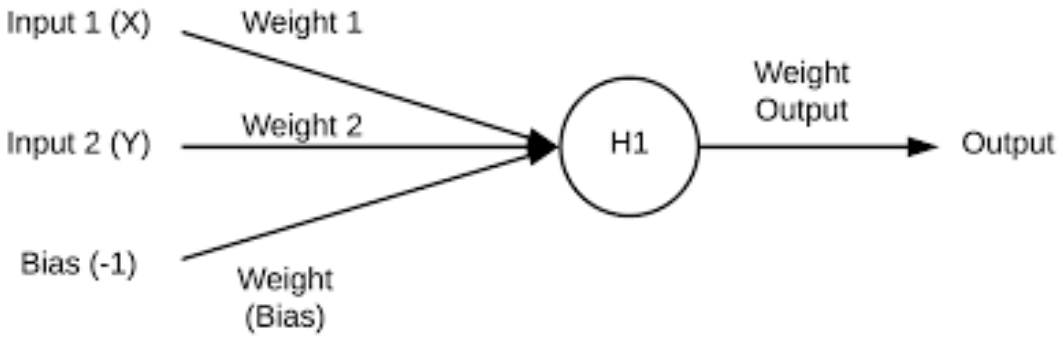

Figure 8: Radial Basis Function

The radial basis function neural network is applied extensively in power restoration systems. In recent decades, power systems became bigger and more complex. This increases the danger of a blackout. This neural network is employed within the power restoration systems so as to revive power within the shortest possible time.

iii. Multilayer Perceptron

A multilayer perceptron has three or more layers. It's wont to classify data that can't be separated linearly. It's a kind of artificial neural network that's fully connected. This is often because every single node during a layer is connected to every node within the following layer.

A multilayer perceptron uses a nonlinear activation function (mainly hyperbolic tangent or logistic function). Here's what a multilayer perceptron seems like.

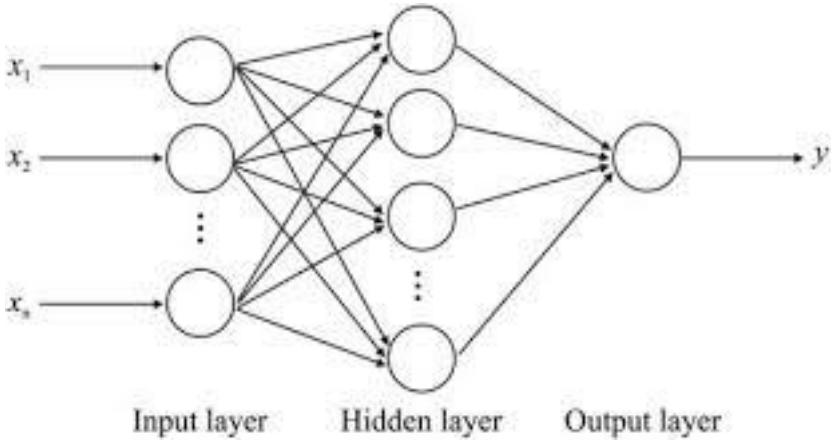

Figure 9: Multilayer Perceptron

This type of neural network is applied extensively in speech recognition and machine translation technologies.

iv. Convolutional Neural Network

A convolutional neural network (**CNN**) uses a variation of the multilayer perceptrons. A CNN contains one or quite one convolutional layers. These layers can either be completely interconnected or pooled. Before passing the result to subsequent layer, the convolutional layer uses a convolutional operation on the input. Thanks to this convolutional operation, the network are often much deeper but with much fewer parameters.

Due to this ability, convolutional neural networks show very effective leads to image and video recognition, tongue processing, and recommender systems. Convolutional neural networks also show great leads to semantic parsing and paraphrase detection. They're also applied in signal processing and image classification.

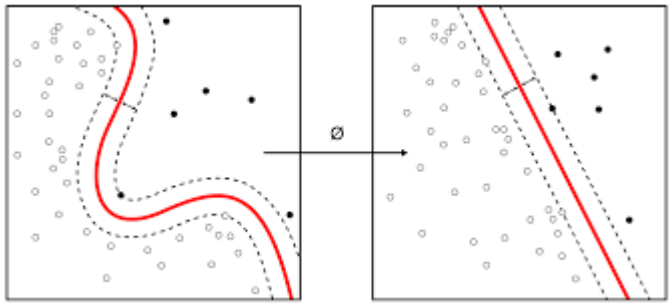

Figure 10: Convolutional Neural Networking

v. Recurrent Neural Network

A Recurrent Neural Network may be a sort of artificial neural network during which the output of a specific layer is saved and fed back to the input. This helps predict the result of the layer. The first layer is made within the same way because it is within the feedforward network. That is, with the merchandise of the sum of the weights and features. However, in subsequent layers, the recurrent neural network process begins.

From each time-step to subsequent, each node will remember some information that it had within the previous time-step. In other words, each node acts as a memory cell while computing and completing operations.

The neural network begins with the front propagation as was common but remembers the knowledge it's going to got to use later.

If the prediction is wrong, the system self-learns and works towards making the proper prediction during the backpropagation. This sort of neural network is extremely effective in text-to-speech conversion technology. Here's what a recurrent neural network seems like.

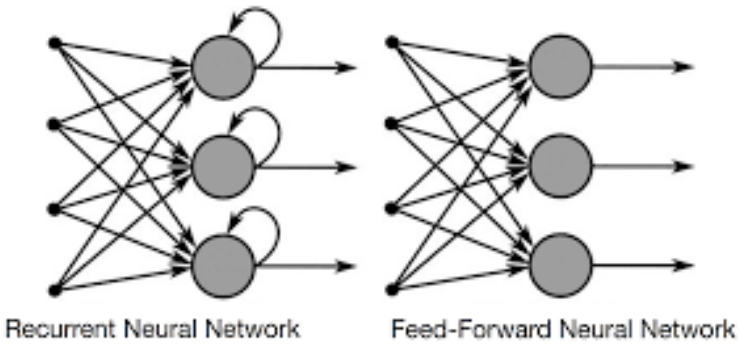

Figure 11: Recurrent Neural Network comparison

vi. Modular Neural Network

A modular neural network features a number of various networks that function independently and perform sub-tasks. The various networks don't really interact with or signal one another during the computation process. They work independently towards achieving the output.

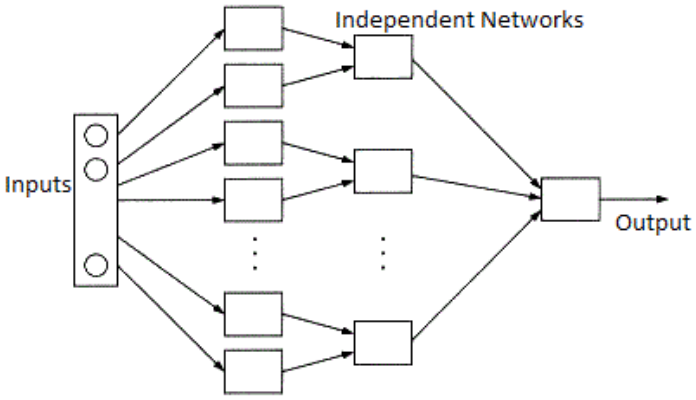

Figure 12: Modular Neural Network

As a result, an outsized and sophisticated computational process are often done significantly faster by breaking it down into independent components. The computation speed increases because the networks aren't interacting with or maybe connected to every other. Here's a visible representation of a Modular Neural Network.

vii. Sequence- To- Sequence Model

A sequence to sequence model consists of two recurrent neural networks. There's an encoder that processes the input and a decoder that processes the output.

The encoder and decoder can either use an equivalent or different parameters. This model is especially applicable in those cases where the length of the input file isn't an equivalent because the length of the output data. Sequence-to-sequence models are applied mainly in chatbots, MT, and question answering systems.

Neural Network Design/Architecture

The term neural network design refers to the arrangement of neurons into layers and therefore the connection patterns between layers, activation functions, and learning methods. The neural network model and therefore the design of a neural network determine how a network transforms its input into an output.

Advantages of Neural Networks

i. Neural Networks have the power to find out by themselves and produce the output that's not limited to the input provided to them.

ii. The input stored in its own networks, hence the loss of

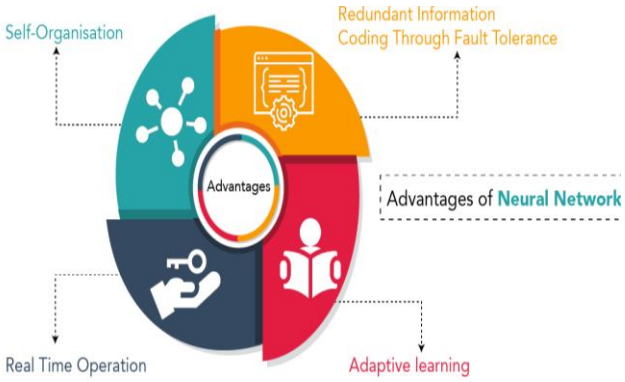

Figure 13: Advantages of ANN

knowledge doesn't affect its working.

iii. Neural Network Multi-Functionalities.

iv. These networks can learn from the examples and apply them when the similar events arise making them ready to run through real-time events.

v. If a neuron isn't responding or a bit of data is missing, the network detects the fault and still produces the output.

vi. They can perform multiple tasks in parallel without affecting the system performances

Disadvantages of Neural Networking

i. Artificial neural networks require processors with multiprocessing power, in accordance with their structure. For this reason, the belief of the equipment depends.

ii. Unexplained behavior of the network is that the most vital problem of ANN. When ANN produces a probing solution, it doesn't provide a clue on why and the way. This reduces trust within the network.

iii. Determination of proper network structure is difficult. There's no specific rule for determining the structure of artificial neural networks. Appropriate network structure is achieved through experience and trial and error.

iv. Difficulty of showing the matter to the network is that the main disadvantage of neural. ANNs can work with numerical information. Problems need to be translated into numerical values before being introduced to ANN. The display mechanism to be determined here will directly influence the performance of the network. this relies on the user's ability.

Applications of Neural Networking

Neural networks are successfully applied to the broad spectrum of data-intensive applications. due to their ability to breed and model nonlinear processes, Artificial neural networks have found applications in many disciplines. Application areas include system identification and control like vehicle control, trajectory prediction, process control, natural resources management, quantum chemistry, general game playing, pattern recognition radar systems, face identification, signal classification, 3D

reconstruction, visual perception and more, sequence recognition, gesture, speech, handwritten and printed text recognition), diagnosis , finance .e.g. automated trading systems, data processing , visualization, MT , social network filtering and e-mail spam filtering. ANNs are wont to diagnose cancers, including carcinoma, prostatic adenocarcinoma, colorectal cancer and to differentiate highly invasive neoplastic cell lines from less invasive lines using only cell shape information.

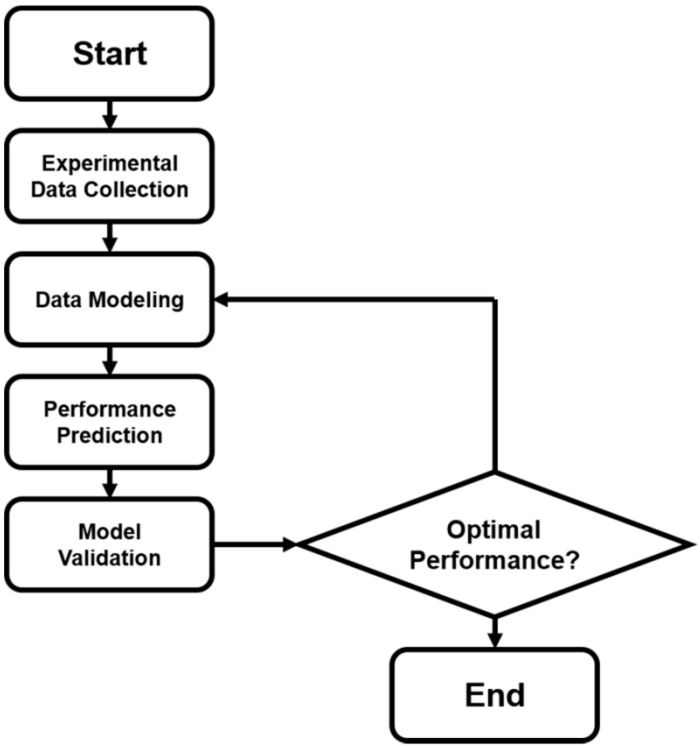

Figure 14: Application of ANN

ANNs are wont to accelerate reliability analysis of infrastructures subject to natural disasters and to predict foundation settlements. ANNs have also been used for building black-box models in geosciences hydrology, ocean modeling and coastal engineering, and geomorphology. ANNs are employed in cybersecurity, with the target to discriminate between legitimate activities and malicious ones. For instance, machine learning has been used for classifying Android malware, for identifying domains belonging to threat actors and for detecting URLs posing a security risk. Research is underway on ANN systems designed for penetration testing, for detecting botnets, credit cards frauds and network intrusions.

ANNs are proposed as a tool to simulate the properties of many-body open

quantum systems. In brain research ANNs have studied short-term behavior of individual neurons, the dynamics of neural circuitry arise from interactions between individual neurons and the way behavior can arise from abstract neural modules that represent complete subsystems. Studies considered long-and short-term plasticity of neural systems and their reference to learning and memory from the individual neuron to the system level.

Some of the major applications of neural networking are as follow:

1. **Machine Translation:**
   Machine translation software is employed round the world despite its limitations. In some domains, the standard of translation isn't good. To enhance the results researcher, try different techniques and models, including the neural network approach. The aim of Neural-based MT for Medical Text Domain study is to examine the consequences of various training methods on a Polish-English MT system used for medical data. To coach neural and statistical network-based translation systems the ecu Medicines Agency parallel text corpus was used.

2. **Character Recognition:**
   Character Recognition systems even have numerous applications like receipt character recognition, invoice character recognition, character recognition, legal billing document character recognition, and so on. The article Character Recognition Using Neural Network presents a way for the popularity of handwritten characters with 85% accuracy.

3. **Fraud Detection:**
   Fraud detection is important for any economic system. However, the way of committing frauds and also for detecting them have evolved considerably within the lasts years, mainly due the event of latest technologies. Therefore, fraud detection via statistical schemes has become a crucial tool to scale back the probabilities of frauds. Artificial Neural Networks (ANN) are applied for fraud detection, mainly within the context of supervised classification. In, ANN is applied for credit card fraud detection. The utilization of ANN for fraud detection is completed using the generated network as a classifier. With this approach, the network is trained with samples of fraud ulentand non-

fraudulent actions. Once trained, the ANN is in a position to classify new data as fraudulent or non-fraudulent activities.

4. **Target Marketing:**
   Database marketing uses the facility of knowledge and knowledge technology within the pursuit of private marketing of products and services to consumers, supported their preferences and wishes. Artificial Neural Networking sets up the self- learning functionalities within the machine such the commercial enterprise can study about the market detail. It furthermore classifies the present demands and approaches of individuals that motivates commercial enterprise and make a lot of profit out of it.

5. **Target Recognition:**
   The use of the ANN isn't limited. During late 2000's it's been widely utilized in the world of the military. Automatic target recognition and detection system has been developed for the defense reaction and for security purpose. These systems use the self-learning and interconnected neural system that works in military environment. It helps to trace the target deploy the missiles and control over security breach of any protocol.

6. **Medical Field:**
   An extensive amount of data is currently available to clinical specialists, starting from details of clinical symptoms to varied sorts of biochemical data and outputs of imaging devices. Each sort of data provides information that has got to be evaluated and assigned to a specific pathology during the diagnostic process. To streamline the diagnostic process in daily routine and avoid misdiagnosis, AI methods (especially computer aided diagnosis and artificial neural networks) are often employed. These adaptive learning algorithms for this procedure is obtain through the neural networking environment which will handle diverse sorts of medical data and integrate them into categorized outputs.

Cyber Security

Introduction

Figure 15: Cyber Security

Cybercrime may be a global problem that's been dominating the news cycle. It poses a threat to individual security and a good bigger threat to large international companies, banks, and governments. Today's organized cybercrimes far out shadow lone hackers of the past now large gangland rings function like start-ups and sometimes employ highly-trained developers who are constantly innovating online attacks. With such a lot data to take advantage of out there, Cybersecurity has become essential.

What is Cybersecurity?

Cybersecurity refers to a group of techniques wont to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

From a computing point of view, security comprises cybersecurity and physical security both are employed by enterprises to guard against unauthorized access to data centers and other computerized systems. Information security, which is meant to take care of the confidentiality, integrity, and availability of knowledge, may be a subset of cybersecurity. the utilization of cyber security can help prevent cyber-attacks, data breaches, and fraud and may aid in risk management.

Some Major Incidents on Cyber Attack in History

1. **1988 – The First: The Morris Worm**
   The first cyber-attack began with good intentions and ended with unexpected consequences. In 1988, Cornell University grad student, Robert Tappan Morris, developed a program to assess the dimensions of the web. The program would crawl the online, install itself on other computers, and then count what percentage copies it made. Once tallied, the results would indicate the amount of computers connected to the web

history of cyber-attacks. Unfortunately, problems arose for Morris, who struggled to make sure accuracy. Morris made a command that forced the worm to put in itself on a computer all out of seven times, albeit the pc claimed it already had the program. With each installation, the infected computers would become further debilitated until they finally crashed. it had been the primary Distributed Denial of Service (DDoS) attack, and it had been entirely accidentally.

In total, the worm damaged approximately 6,000 computers (10% of the whole internet at the time). The estimated cost of repairing the consequences of the worm range between $100,000 and $1 million or between $201,000 and $2.9 million adjusted for inflation. Morris was charged with the violation of the pc Fraud and Abuse Act, and his sentence included fines, plus three years of probation and community service.

2. **1995 – LA KIIS FM Porsche**

   In an amusing cyber-attack, Kevin Poulsen used his hacking ability to cheat during a radio contest. LA KIIS FM was making a gift of a Porsche to the 102nd caller, and Poulsen naturally wanted to win. He infiltrated the phone network to dam their ability to receive calls, so Poulsen was assured the 102nd caller slot. Despite winning the Porsche, he was eventually caught and sentenced to 5 years in prison.

3. **Teen hacks NASA and US Defense Department**

   The year was 1999. Jonathan James was 15 at the time but what he did that year secured him an area within the hacker's hall of fame.

   James had managed to penetrate the computers of a US Department of Defense division and installed a 'backdoor' on its servers. This allowed him to intercept thousands of internal emails from different government organizations including ones containing usernames and passwords for various military computers.

4. **North Korea Cyber Attack on Sony Pictures**
   On November 24, 2014, a hacker group which identified itself by the name "Guardians of Peace" leaked a release of confidential data from the film studio Sony Pictures. the info included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the corporate, copies of then-unreleased Sony films, plans for future Sony films, scripts surely films and other information. The perpetrators then employed a variant of the Shamoon wiper malware to erase Sony's computer infrastructure.

During the hack, the group demanded that Sony withdraw its then-upcoming film The Interview, a comedy a few plot to assassinate North Korean leader Kim Jong-un, and threatened terrorist attacks at cinemas screening the film. After many major U.S. cinema chains opted to not screen The Interview in response to those threats, Sony elected to cancel the film's formal premiere and mainstream release, opting to skip on to a downloadable digital release followed by a limited theatrical release subsequent day.

Importance of Cyber Security

Cyber security plays a great role in the present technical era. The following are the major role and importance of cyber security to secure,

- communication systems, like emailing, phone calls and messages
- transportation systems, including controlling traffic, navigation system of airplanes,
- government databases, including Social Security numbers, licenses, tax records
- financial systems, including bank accounts, loans and paychecks,
- medical systems, including equipment and medical records
- Educational systems, including grades, report cards and research information etc.

Types of Cyber Security

Cyber security is that the state or process of protecting and recovering networks, devices and programs from any sort of cyberattack. There are many types of cyber security and to be better protected each type should be well known. The various types of cyber security are as follows:

a) **Critical infrastructure security:** It consists of cyber-physical systems such as electricity grid and water purification systems.

b) **Network Security:** It protects internal networks from intruders by securing infrastructure.

c) **Application security:** It uses softwares and hardwares to be protected against external threats which may present themselves in the development stage of an application. Its some of the examples are antivirus programs, firewalls and encryption.

d) **Information security:** It protects both physical and digital data in any form from unauthorized access, use, change, disclosure, deletion, or other sorts of malintent.

e) **Cloud security:** A software-based tool that protects and monitors your data within the cloud, to assist eliminate the risks related to on-premises attacks.

f) **Data loss prevention:** It develops policies and processes to handle and prevent the loss of data, and develop recovery policies within the event of a cyber security breach. It controls setting network permissions and policies for data storage.

g) **End-user education:** It acknowledges that cyber security systems are only as strong as their potentially weakest links: the folks that are using them. End-user education teaches users to follow best practices like not clicking on unknown links or downloading suspicious attachments in emails—which could let in malware and other kinds of malicious software.

Cyber Threats

A cyber or cybersecurity threat could be a malicious act that seeks to wreck data, steal data, or disrupt digital life generally. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks etc.

Cyber threats also ask the likelihood of a successful cyber attack that aims to realize unauthorized access, damage, disrupt, or steal an information technology, network, property or the other sort of sensitive data. Cyber threats can come from within a corporation by trusted users or from remote locations by unknown parties.

Types of Cyber Threats

There are many sorts of cyber threats which will attack your devices and networks, but they typically fall under three categories.

The categories are attacks on confidentiality, integrity and availability.

1. **Attack on confidentiality:** These attacks are often designed to steal the personal identifying information and your bank account or MasterCard information. Following these attack, your information are often sold or traded on the dark web for others to get and use.

2. **Attack on integrity:** These attacks contain personal or enterprise sabotage, and are often called leaks. A cybercriminal will access and release sensitive information for the aim of exposing the info and influencing the general public to lose trust during a person or a corporation.

3. **Attacks on availability:** The aim of this sort of cyberattack is to dam users from accessing their own data until they pay a fee or ransom. Typically, a cybercriminal infiltrates a network and authorized parties from accessing important data, demanding that a ransom be paid.

Companies sometimes pay the ransom and fix the cyber vulnerability afterward in order that they will avoid halting business activities.

The followings are some of the examples explained briefly of cyber threats that fall under the three categories which are listed and explained above.

One of the kind of attack on confidentiality that is social engineering is that the process of psychologically manipulating people into performing actions or making a gift of information. Phishing attacks are the foremost common sort of social engineering.

Phishing attacks usually are available the shape of a deceptive email with the goal of tricking the recipient into making a gift of personal information.

APTs (advanced persistent threats), a kind of attack on integrity, where an unauthorized user infiltrates a network undetected and stays within the network for an extended time. The APT intents to steal data and does not harm the network. APTs often happen in sectors with high-value information, like national defense, manufacturing, and therefore the finance industry.

Malware, or malicious software, may be a sort of attack on availability. It refers to software that's designed to realize access to or damage a computer without the knowledge of the owner. Malware can do everything from stealing your login information and using your computer to send spam, to crashing your computing system. Several common sorts of malware include spyware, keyloggers, true viruses etc.

Figure 16: Malware

Ransomware, another sort of malicious software, is also a kind of attack on availability. Its goal is to lock and encrypt your computer or device data essentially holding your files hostage and then demand a ransom to revive access. A victim typically must pay the ransom within a group amount of

your time or risk losing access to the knowledge forever. Common sorts of ransomware include crypto malware, lockers and scareware.

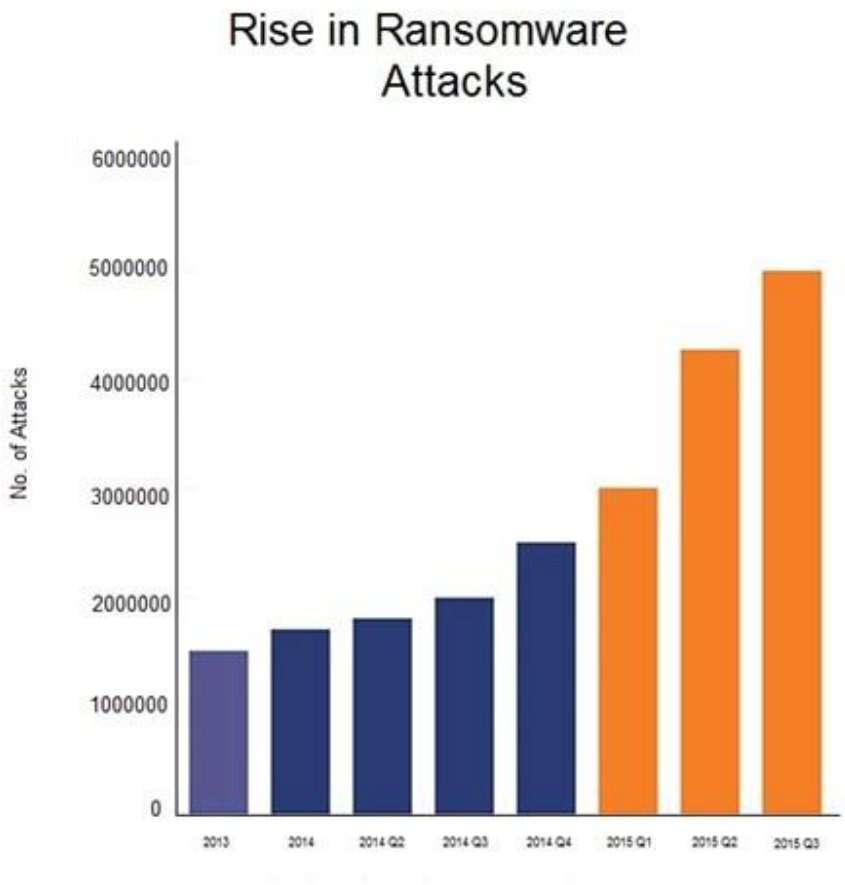

Figure 17: Rise in ransomware attack

Scale of the Cyber Threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk-Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

Prevention from the Cyber Security Threats

Here are some of the best methods that one should apply to prevent themselves from the threats of cyber-crime:

i. Install, use and frequently update antivirus and antispyware software on every computer utilized in your business.
ii. Use a firewall for your Internet connection.
iii. Download and install software updates for your operating systems and applications as they become available.
iv. Make backup copies of important business data, knowledge and personal information.
v. Control physical access to your computers and network components.
vi. Secure your Wi-Fi networks. If you've a Wi-Fi network for your workplace confirm it's secure and hidden.

Evolution of Cyber Security

During the mid to late 2000s, the availability of more complex attack tools became widespread and attack platforms capable of executing many attacks against vulnerable systems were readily available. These attack platforms were able to deliver a replacement kind of attack, mentioned as ‘Buffer Overflows’, against a vulnerable machine and inject payloads which may execute during a successful attack. When utilized together with multiple security evasion techniques, many Intrusion Prevention Systems (IPS) were found to be less effective than vendors claimed. Today, there is a spread of readily downloadable scripts and compiled code capable of executing highly complex attack scenarios.

Identifying and blocking the ‘known’ attack will always have its place, but systems will need to evolve to satisfy the complexity of today’s malicious activity. this needs identifying mutated or evolved ‘known’ exploits, also as identifying new threats yet to be classified and blocked by traditional security defense solutions. A new generation of cyber defense solutions is therefore emerging to satisfy today’s threats.

These sophisticated systems are capable of gathering transmission characteristics from network devices and generating their own behavioral intelligence. This allows complex queries to be run to identify device or user behavior that's indicative of a threat or other malicious activity. These systems operate by trying to seek out transmission characteristics in network traffic that are so unusual when compared with the majority of usual or benign traffic. The traffic is then further scrutinized for behavioral characteristics which may be indicative of a threat.

For an example, if a machine is identified as accepting a replacement connection then immediately establishes a high volume of multiple simultaneous connections to external addresses, which haven't been communicated with historically, this behavior would be identified by a next generation system as malware execution and propagation. This new capability to use powerful and complicated queries against current and historical device and user behavior is highly effective at identifying behavior indicative of malicious activity.

Bibliography

During the completion of this project work, we have used some external sources to cover the required content sufficiently. The reason for this is in some of the topics, we didn't have knowledge about that at all. So in order to complete the project work on the given topic we made some research work from internet. Followings are the major websites or references from where we covered the content:

- ✓ https://towardsdatascience.com/artificial-neural-networks-for-total-beginners-d8cd07abaae4
- ✓ https://medium.com/swlh/learning-paradigms-in-neural-networks-30854975aa8d
- ✓ https://www.digitalvidya.com/blog/types-of-neural-networks/
- ✓ https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
- ✓ https://www.researchgate.net/
- ✓ https://www.geeksforgeeks.org/

- ✓ https://www.digitalistmag.com/